SIGNAL TELCOM PARTNERS®

1180 Golden Hills Road
Colorado Springs, CO 80919
v-(719) 532-0452
f-(720) 222-1984

February 15, 2010

via electronic submission

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street S. W., Suite CY-B402
Washington, D.C. 20554

RE: RYE TELEPHONE COMPANY
Certification of CPNI Filing, March 1, 2010
FCC Docket EB 06-36
EB-06-TC-060

Dear Ms. Dortch,

In accordance with the Public Notice issued by the Enforcement Bureau on January 15, 2010 (DA 10-91), please find attached **Rye Telephone Company's** annual compliance certificate for the most recent period, as required by section 64.2009(e) of the Commission's Rules, together with a statement of how its operating procedures ensure that it is or is not in compliance with the rules (Attachment), an explanation of actions taken against data brokers, and a summary of customer complaints received in the past year concerning the unauthorized release of Customer Proprietary Network Information (CPNI).

Should you have any questions regarding this filing, please do not hesitate to give me a call.

Sincerely,

JOVANKA MERSMAN
Tariff/Regulatory Manager

JM/jam
Enclosures
cc: Best Copy and Printing, Inc., via email FCC@BCPIWEB.COM

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for	2010 covering the prior calendar year 2009
Date filed:	February 15, 2010
Name of company(s) covered by this certification:	Rye Telephone Company
Form 499 Filer ID:	805392
Name of signatory:	David Shipley
Title of signatory:	Vice President

I, David Shipley, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

RYE TELEPHONE COMPANY

BY _____

David Shipley
Vice President
PO Box 19048
Colorado City, CO 81019
(719) 676-3131

ATTACHMENT: Statement of Compliance with CPNI Rules

STATEMENT OF COMPLIANCE WITH CPNI RULES

RYE TELEPHONE COMPANY (the "Company") has implemented the following procedures to ensure that it is compliant with part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training;

The Compliance Officer arranges for the training of all employees on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. Employees are informed as to where the Company's CPNI manual with rules is kept in the office.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees.

A copy of the Company's disciplinary process is kept in the CPNI manual.

Customer Notification and Request for Approval to Use CPNI

The Company provided "Opt Out" notification to its customers. If the customer does not object within the thirty (30) day waiting period, the customer is deemed to have consented to use of his/her CPNI. Regardless, the Company will not share the customer's CPNI with any joint venture partner, independent contractor or any other third party without customer affirmative express consent. For marketing purposes, the Company does mass marketing to all customers, or uses CPNI to market only service offerings among the categories of service to which the customer already subscribes.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed so that employees can readily identify customers that have restricted the use of their CPNI.

For the customers that have opted-out and said the Company cannot use their CPNI, that decision will remain valid until the customer changes it.

The company sends the opt-out notice every two years to those customers that have not previously opted out.

The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

A copy of the most recent notification is kept in the CPNI official files.

Marketing Campaigns

If the Company uses CPNI for any marketing campaign, the Compliance Officer will review the campaign and all materials to ensure that it is in compliance with CPNI rules.

The Company has a process for maintaining a record of any marketing campaign of its own, or its affiliates, which uses customer's CPNI.

Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

In-office visit – the customer must provide a valid photo ID matching the customer's account information.

Customer-initiated call – the customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

If the customer wants to discuss call detail information that requires a password, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Company will continue its routine customer care procedures.

- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Address of record.

The notification to the customer will be sent to the address (postal or electronic) of record.

The Company has a process for tracking when a notification is required and for recording when and how the notification is made. Employees generate a notice and a copy of the notice is kept in Company official files.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at hppt://www.fcc.gov/eb/cpni.

- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Summary of Consumer Complaints

There were no consumer complaints regarding unauthorized release of CPNI in previous year.

Action against Data Brokers

There were no actions taken against data brokers or pretexters for unauthorized access to CPNI in the previous year.

Record Retention

The Company retains all information regarding CPNI in the Company's official files. Following is the minimum retention period we have established for specific items:

- CPNI notification and records of approval – one year
- Marketing campaigns – one year
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years